TRANSPUTEC

macOS Management with Microsoft Intune

Microsoft
Solutions Partner

What is it?

macOS Management with Microsoft Intune helps integrate Apple devices into an existing Microsoft Intune setup. It makes it easier to manage all devices, even when they use different operating systems. This approach keeps company data secure, ensures compliance, and improves efficiency when managing macOS devices.

The service includes:

→ **Prerequisites:**

Requires an M365 license (Business Premium, E3, or E5) with Intune and registration in Apple Business Manager.

→ **Device Management:**

Manage both company and personal macOS devices with full control and flexibility.

→ **Compliance:**

Apply compliance policies and Conditional Access to keep devices secure.

→ **Device Settings:**

Configure features, restrictions, and network profiles in detail.

→ **Security:**

Enhance protection with firewall, Gatekeeper, and FileVault settings.

→ **App Deployment:**

Quickly deploy key apps like M365, Edge, Defender, and other supported packages (Line of Business, DMG, PKG).

Why you need it?

Organisations often face several challenges in managing macOS devices within their IT infrastructure, leading to potential security vulnerabilities, compliance issues, and operational inefficiencies. This solution directly addresses these concerns by extending the robust management capabilities of Microsoft Intune to macOS devices.

macOS Management with Microsoft Intune helps you avoid these problems.

→ **Clarifying Intune's Capability:**

Intune manages both Windows and macOS devices, providing a unified endpoint management approach.

→ **Expanding Coverage:**

Extends existing Intune deployments to include unmanaged macOS devices for consistent policy enforcement and security.

→ **Maximising M365 Value:**

Enables full use of M365 licenses (such as Business Premium) by applying Intune features to Apple devices.

→ **Improving Security and Compliance:**

Enforces policies, configures endpoint security, and applies Conditional Access to reduce risks.

→ **Simplifying Operations:**

Automates enrolment and onboarding while improving user experience and productivity.

Get started today!

- Schedule a free consultation << Click here >>
- or just give us a call on: +44 (0) 20 8584 1400.

Why you need us?

→ **Intune Expertise:**

Skilled in deploying Intune across Windows, macOS, Android, and iOS for unified device management.

→ **macOS Integration:**

Extend Intune to unmanaged macOS devices, bringing all endpoints under one system.

→ **User Experience:**

Offer lightweight management options that keep security strong while remaining user-friendly.

→ **Full Control:**

Enable detailed configuration of settings, security, and app deployment to match your needs.

→ **Structured Delivery:**

Use a clear process discovery, design, build, test, and go-live—for smooth, efficient rollout.

Company-owned device

Managing company-owned macOS devices with Microsoft Intune provides a robust framework for IT administrators to ensure security, compliance, and a seamless user experience from initial setup to ongoing maintenance. The process is designed to be efficient and comprehensive, covering various aspects of device lifecycle management.

Key aspects of managing company-owned macOS devices include:

- **Automated Enrolment:**
  Devices can be automatically added to Intune, reducing manual setup and correct configuration from day one.
- **Simplified Onboarding:**
  The onboarding process is smooth and efficient, helping users get started quickly with minimal IT assistance.
- **Identity-Based Single Sign-On (SSO):**
  Users enjoy secure, seamless access to apps and services using their existing corporate credentials.
- **Access to Applications and Web Services:**
  Intune enables quick deployment and access to all required business apps and web resources, improving productivity.
- **Extended Configuration Options:**
  Beyond basic setup, administrators can apply detailed configurations to meet company standards and policies.
- **Comprehensive Management Controls:**
  IT teams maintain full control over device settings, security configurations, and app management to ensure compliance.
- **Broad App Package Support:**
  Intune supports multiple app formats, including Line of Business, DMG, and PKG files, offering flexibility in application deployment.

Device enrolment experience

The device enrolment experience for macOS with Microsoft Intune is designed to be user-friendly and efficient, guiding the end-user through a series of steps to integrate their device into the managed environment. This process ensures that devices are properly configured, secured, and ready for corporate use at any environment.

The streamlined device enrolment experience typically involves:

- **Initial Setup:**
  Users complete the basic macOS setup, including language, region, Wi-Fi, and password configuration.
- **Authentication:**
  Users sign in with their Microsoft work or school account, linking the device to Azure Active Directory and Intune.
- **Device Linking:**
  After authentication, the Mac automatically connects to Intune, allowing policies, apps, and settings to be applied.
- **App Installation:**
  Intune deploys and installs required applications, giving users immediate access to essential tools.

Security compliance

Maintaining a strong security posture is paramount for any organisation, and Microsoft Intune provides robust capabilities to ensure macOS devices adhere to defined security and compliance standards. Through Intune, administrators can enforce policies that protect device integrity and data confidentiality.

Key aspects of security compliance for macOS devices include:

- **System Integrity Verification:**
  Intune checks macOS devices to ensure key security features are active and working.
- **OS Version Enforcement:**
  It enforces minimum OS versions so all managed Macs run supported, secure builds.
- **OS Version Enforcement:**
  It enforces minimum OS versions so all managed Macs run supported, secure builds.
- **Strong Password Policy:**
  Intune requires complex passwords to protect device access and sensitive data.
- **Device Encryption:**
  It enforces full disk encryption (e.g., FileVault) to secure stored data from unauthorised access.

Common challenges

Organisations frequently encounter several challenges when it comes to managing macOS devices, often stemming from misconceptions or a lack of awareness regarding available solutions. Addressing these challenges is crucial for effective cross-platform device management.

These common challenges include:

- **Misconception of Intune's Scope:**
  Many think Intune only manages Windows devices, overlooking its strong macOS capabilities and causing fragmented management.
- **Unmanaged macOS Devices:**
  Many organisations have a significant number of macOS devices that remain unmanaged by Intune, creating security gaps and inconsistencies in policy enforcement across their device fleet.
- **Underused M365 Licenses:**
  Organisations with M365 plans that include Intune often miss its macOS management benefits, wasting built-in security and efficiency tools.
- **Privacy and Lockdown Concerns:**
  There is a common misconception that Intune management will lead to excessive device lockdown or an invasion of end-user privacy. It is important to clarify that controls can be applied judiciously, often targeting only company data and resources, thereby respecting user privacy while maintaining corporate security.

Our service offerings

Transputec provides a comprehensive suite of services designed to facilitate and optimise macOS management using Microsoft Intune. Our offerings are tailored to meet diverse organisational needs, from initial implementation to extending existing management capabilities.

Our core service offerings include:

→ **Intune Device Management Implementation:**

We assist organisations in implementing Microsoft Intune for a wide range of devices, including Windows, macOS, Android, and iOS. This ensures a unified and consistent approach to endpoint management across your entire IT ecosystem.

→ **Extension of macOS Management:**

For clients who already utilise Intune for other platforms, we specialise in extending these existing capabilities to currently unmanaged macOS devices. This ensures that all Apple devices are brought under the same robust management framework.

→ **Lightweight macOS Device Management:**

We offer an optional lightweight macOS device management approach that prioritises an excellent end-user experience without compromising on security. This balanced strategy ensures that security measures are effective yet minimally intrusive, promoting user satisfaction and productivity.

Approach and indicative timeline

Our approach to implementing macOS management with Microsoft Intune is structured and phased, designed to ensure a smooth transition and effective deployment.

The indicative timeline for this process is as follows:

Phase	Duration
Discovery and Due Diligence	1 day
Design Phase	1 day
Build Phase	3 day
Test and Pilot	3 day
Go-Live and Early Life Support	2 day